Abstract

We present Obscuro, a decentralised Ethereum Layer-2 Rollup protocol designed to achieve privacy, scalability and prevent Maximal Extractable Value.

The design of Obscuro ensures that existing Ethereum apps can move over to Obscuro for virtually no cost. Any developer familiar with Ethereum can build privacy-preserving apps on Obscuro that benefit from the adoption, legitimacy, security, developer tooling and liquidity of the entire Ethereum ecosystem.

End-users can continue to use MetaMask or their favourite Ethereum wallet. Interacting with an Obscuro application is the same as interacting with any Ethereum application. With a seamless user and developer experience, Obscuro changes the paradigm around privacy on the blockchain.

Obscuro leverages a pragmatic technology for encrypting the ledger, Trusted Execution Environments (TEEs). TEEs provide robust confidentiality guarantees with certainty over the code running. They allow Obscuro to offer smart contracts, decentralisation, scalability and privacy in a way other privacy providing techniques cannot.

Obscuro uses Confidential Rollups, a new type of roll-up inspired by existing roll-up-based L2 offerings Optimistic and ZK Rollups. The use of confidential computing techniques and economic incentives allows Obscuro to retain the performance and programming model simplicity of Optimistic roll-ups and attain confidentiality, short withdrawal periods, and address MEV.

Example Use Cases

Obscuro supports transactional and computational privacy, which opens up a whole new world of use-cases.

Sealed Bid Auction

In a sealed bid auction, bidders privately submit their one best offer in writing in a sealed envelope. The bids are opened privately by the auctioneer and seller. They do not reveal the bids to any of the participants.

Keeping the bids private helps ensure that if all bids are too low for any of them to be accepted by the seller, the property is not stigmatised by having a perceived low value in the marketplace. It also ensures that the auctioneer cannot collude and reveal a competing bid to another bidder privately or front-run a bidder and out-bid them.

We explore here how the outcome of the ConstutionDAO experiment could have been vastly different with the use of Obscuro.

Dark pools and OTC Trading

A dark pool is a privately organised exchange for trading securities where exposure is hidden until after execution and reporting. This allows investors to trade without publicly revealing their intentions during the search for a buyer or seller and hiding any pricing data, which could result in investors receiving poorer prices.

Dark pools on Obscuro would be different from a typical DEX; direct peer-to-peer trading with a layer of 'dark' price discovery added.

Prices for assets can be derived from order flow within the Obscuro enclaves, guaranteeing fair price discovery and leveraging oracles such as Chainlink to ensure prices are within a fair band. The eventual revelation is also essential, as trades eventually must be disseminated to all investors (a consolidated tape).

Over-the-counter (OTC) trading is where bespoke products are tailored to specific client requirements. The most common usage of OTC is in financial derivatives, where "OTC" means the opposite of "Exchange-traded".

They come in where there is a need for unique, idiosyncratic terms for, as an example, an option, such as non-standard length of time, strike price, market conventions, or payoff structure and are negotiated between a buyer and issuer. Obscuro can guarantee privacy in both negotiating and structuring such products.

This type of trading is made possible with Obscuro.

Commercial agreements

Commercial agreements, such as a Service Level Agreement (SLA) between a supplier and buyer, are incredibly sensitive. They reveal commercial relationships and impact reputation where an SLA has failed. Agreements deployed to Obscuro can be entirely private, such that aside from the participants, nobody even knows the contract exists. These commercial agreements on Obscuro ushers in more efficient handling of automated payouts based on independently verified data supplied by oracles.

Shapeshifting NFTs

Obscuro provides an entirely new and compelling experience for NFT artists and holders.

With Obscuro, artists can create an NFT that initially appears mundane or common, but a secret is embedded in the smart contract. When this secret is triggered by an external event like a full moon in Tasmania, the NFT changes to something rare and exciting, potentially collaborating with another well-known NFT collection or unlocking an entirely different reward, such as hidden crypto. This is an entirely new way for artists to engage with their audience.

The unknown embedded within the Obscuro also provides for an entirely new dimension in NFT speculation.

Gaming

Games that rely on player actions and positions being secret are impossible on today's transparent blockchains without computational privacy. With Obscuro, games such as Civilisation, Starcraft and other "fog of war" type games become a reality. The paradigm can begin to shift from "Play to Earn' to 'Pay to Play' as AAA games start to emerge with embedded NFTs are crypto prizes that are kept hidden, with absolute certainty, even from the developers of the games.

Obscuro public events

Ethereum application developers can use a confidential L2 like Obscuro for some jobs that are not possible otherwise.

For example, an L1 smart contract organises a fair lottery that needs a reliable random number generator that the miners cannot game.

Another example is publishing the result of a poker game played inside Obscuro, which the L1 contract can use to make a payment or update the tournament results.

The challenge for achieving this functionality is that the data originating in L2 has to be final. Luckily Obscuro has this mechanism already in place for processing withdrawals.

Obscuro introduces

Obscuro introduces a new type of roll-up called 'Confidential roll-ups'. When combined with the POBI protocol, they provide several advantages over existing Layer-2s and other privacy networks:

- Unlike other Layer-2s, Obscuro is trustless and decentralised from day one. It takes processing from the Ethereum Layer-1 (L1) and allows lower transaction costs similar to other Layer-2 (L2) networks.
- All transaction intentions on Ethereum are visible to everyone. However, Obscuro keeps all transactions and the internal state of application contracts encrypted and hidden.
- Front runners rely on transactions being out in the open to achieve MEV at the end user's expense. Given that Obscuro keeps all transactions and the internal state of application contracts encrypted, MEV is eradicated
- By providing an encrypted Ethereum Virtual Machine (EVM), deploying existing Ethereum smart contracts to Obscuro is trivial.
- Obscuro leverages TEEs for privacy but not for integrity and is not affected by the limitations of hardware-based confidential computing.
- Obscuro guarantees quick finality by synchronising the publishing of roll-ups to the cadence of the L1 blocks.
- Obscuro solves the long withdrawal problem seen in fraud-based roll-ups (Optimistic).
- The user experience is critical to the success of Obscuro and privacy networks in general. Obscuro provides a seamless Ethereum experience for both app developers and end-users. App developers can fork over existing Ethereum applications and build new applications using any of the Ethereum supported programming languages and developer tooling. End users can continue to use Metamask or their favourite wallets. There is no change in their experience.
- Obscuro provides both transactional and computational privacy.
- A fully decentralised bridge between Ethereum and Obscuro backed by the complete security of Ethereum.
- Being entirely decentralised provides a genuine need for a utility token to power the network and provide decentralised governance.

Privacy on Obscuro

The privacy Obscuro provides can be split into transactional and computational privacy.

Transactional privacy

Transactional privacy is the ability to maintain privacy over transactions on the L2. For example, keeping user token balances, participants of a transaction and the amounts transferred private is the main use of transactional privacy.

This is the problem that ZKP-based privacy problems, such as Z-Cash and Aztec Protocol, solve.

Obscuro provides transactional privacy and keeps token contract calls entirely confidential by encrypting transactions from the point of origination, the wallet.

Computational privacy

In addition to transactional privacy, Obscuro also provides a much deeper form of privacy known as computational privacy. This is complete and absolute privacy over the entire computation of smart contracts and the network.

With computational privacy, it's possible to keep inputs and outputs from contracts private and any logic executed within the smart contract. This opens up huge possibilities across DeFi, NFTs, Gaming, DAOs, the Metaverse and things yet to come.

The example of the Commercial Agreement, Gaming and NFT use-cases are only possible with computational privacy.

Trusted Execution Environments

A Trusted Execution Environment is a secure area of a central processor or CPU. It guarantees that code and data loaded inside are protected with respect to confidentiality and integrity as it is processed.

Trusted Execution Environments or TEEs solve a notoriously difficult problem - How to provide secure execution for critically sensitive data?

To solve this problem, TEEs provide the ability to:

- Keep cryptographic key material secret
- Prevent other people from spying or seeing transactions happen, including the owner or operator of the TEE
- Search encrypted, sensitive data
- Sign with cryptographic keys
- Execute code with complete privacy
- Attest to the code to provide guarantees that what you think is running really is running

Solving all of the above is an unsolved problem without the use of TEEs. Zero-knowledge proofs cannot solve this set of problems, and homomorphic encryption is still in its infancy. TEEs provide a pragmatic, elegant solution.

The blog post here presents a great mental model.

Intel SGX

There exist multiple TEE options. These include:

- Intel's platform called Software Guard Extensions, or SGX for short

- AMD's SEV, which is similar to SGX
- ARM's TrustZone, which lives inside the majority of ARM chips

Obscuro focuses initially on Intel's SGX. This decision is based on the depth of the SGX solution and how battle-hardened it has become over the years. In addition, Intel has recently announced they are doubling down on their server-side SGX offerings in response to the huge number of new use-cases arising.

SGX is being employed by Secret Network, Oasis Network, Corda and Avalanche, amongst others in the blockchain space.

Finally, the Obscuro team brings over five years of experience working with SGX in partnership with Intel. In the longer term, to decentralise away this dependency on Intel, Obscuro will expand to other TEE offerings and homomorphic encryption once it evolves further.

Rollups

Roll-ups are fast becoming the de-facto approach to scaling L1 blockchains. They aim to move execution away from the L1 but tie back to it for security, data availability and access to liquidity.

Users engage with contracts on a second-layer network of nodes, where transaction processing work takes place. L2 transactions are verified and posted in compressed form in a single roll-up transaction to the L1 blockchain. An L1 contract provides the bridge between the two and processes deposits and withdrawals.

The two prevalent forms of roll-up today are fraud proofs and validity proofs.

The best-known example of fraud-proof roll-ups is Optimistic roll-ups. They present an optimistic view of the world based on lightweight verification of transactions on the L2. All transactions are assumed to be correct until a user provides a fraud-proof to challenge an invalid transaction. To provide this functionality, a challenge window of seven days (Dispute Time Delay) is provided in which state transaction is considered not final. Actions like withdrawals are delayed until after this window.

The above challenge requires the parties that are part of an invalid transaction to be present (liveness) and engage in an interactive process to resolve the invalid transaction.

The best-known example of validity proof-based roll-ups is Zero-knowledge roll-ups. Similar to Optimistic roll-ups, they verify transactions on the L2 but then generate proof that the transactions are valid and post proof to the L1. While there exist many ways of doing this, ZKPs are leveraged for their succinctness qualities.

Given that ZKPs are used to prove from one user to another that they have information without revealing the specific information, ZKPs are used in the context of L2s to prove to the L1 that a group of transactions are valid without the overhead of providing all of the transactions. Once the L1 has verified the proof provided by the L2, the state transition is made.

It is essential to point out that ZKPs used in this way are not solving any privacy problem, despite the use of 'zero knowledge' in the name. ZKPs are a poor solution to solving privacy problems, as explained here

A disadvantage of ZKPs, compared to Optimistic roll-ups, is that proofs are required for every state transition and not just contested ones. In addition, generating proofs is computationally expensive and must be done off-chain.

Confidential roll-ups

Confidential roll-ups are an innovation in Obscuro that leverages TEEs and the Proof of Block Inclusion (POBI) protocol.

Like those based on fraud and validity proofs, confidential roll-ups move computation off of the L1 and over to the L2.

The problems confidential roll-ups solve include:

- Some L2s have long withdrawal delays. Obscuro solves this as it is not dependent on submitting fraud proofs. Instead, a much smaller time delay window is required to allow for the improbable scenario of every Obscuro node being taken offline and supported TEEs being hacked. This window will eventually settle to be a small number of Ethereum blocks.
- Most L2s in the space require a centralised sequencer/aggregator/proof generator creating a single point of failure. Obscuro is entirely decentralised from day one through TEEs and POBI. Run by its users, Obscuro is unstoppable, uncensorable and will never go down.
- The ability to use the entire Ethereum Virtual Machine as provided by GETH. There is no need to build a custom EVM with limited functionality or a requirement for developers to change how they build Ethereum applications.
- Last but not least, total privacy over the entire L2 by encrypting the ledger.

POBI

Obscuro introduces a novel protocol called Proof of Block Inclusion. It is this protocol that drives the consensus for confidential roll-ups.

The protocol is responsible for:

- Ensuring that roll-up round winners are selected fairly.
- Rewards are fairly distributed to aggregators and verifiers who secure the network.
- Edge cases where the network is compromised only ever result in a temporary pause to withdrawals to protect the network until the protocol resolves the issue

Data revelation

Our hypothesis is that the value of privacy erodes with time. And so, Obscuro introduces a revelation period that allows developers to one of five fixed periods for when data should be made public. Obscuro provides privacy as experienced in the non-blockchain world without building a platform for nefarious activity.

An important insight in this direction is that the value of confidentiality decays over time, to the point where transactions may just be of historical interest. For many transactions involving value, it is critical that they are not public when processed and cannot be front-run (MEV), but for others, they are price-sensitive for a more extended period. Obscuro uses this insight and implements a flexible policy for delayed transaction revelation. The knowledge that transactions become public in the future is a deterrent for users to engage in criminal behaviour because law-enforcement agencies will eventually catch up.

Obscuro transactions are encrypted with different keys representing discrete revelation periods, which can be revealed independently.

Initially, Obscuro has a maximum one-year reveal period for all transactions. In other words, developers can select a revelation period of up to a year.

It can be argued that this is insufficient for some use-cases, e.g. government secrets are kept private for 20-30 years. As such, the decision of the maximum revelation period will eventually fall to the Obscuro community to determine. Including the ability to whitelist some apps to maintain privacy in perpetuity if the community votes on it.

Tokenomics

The network requires the participation of several types of actors, some of whom incur costs in performing their roles and need to be remunerated. Furthermore, the system's security depends partly on the ability to economically punish those who can be proved, within the protocol, to have acted maliciously. This is achieved through a traditional staking model, and a digital asset, OBX, is used for these purposes.

The main goals for the creation of the OBX token are to provide a truly decentralised network and sustainable growth of the network. That means creating an equally attractive system to developers, Obscuro node operators, end-users, enterprises, and the wider community.

The OBX Token will be issued as a utility token. The token has four primary uses:

- During bootstrapping, provide a block reward to incentivise users to operate obscuro nodes.
- A medium in which users can pay fees and node operators receive rewards.
- A means to fund the ongoing development of the Obscuro platform. Other L2s, being centralised, can collect fees through Eth using a central sequencer. Obscuro, being an entirely decentralised network, requires an alternative utility token for funding.
- A way to incentivise ecosystem development via grants and competitions.

Users

Obscuro seeks to improve the experience for three groups. The first is retail users, who enjoy the benefits of DeFi (Decentralised Finance), but find that they are taken advantage of by Ethereum miners or stakers, who can observe their transactions and front-run those which represent profitable trades. Or they are keen to use DeFi, but won't until it provides the same privacy guarantees that TradFi (Traditional Finance) does.

While the cost of visibility of online activity charged by Big Tech in Web2 was exposure to targeted advertisements, in the "Internet of Value" Web3 world, the cost of visibility will be more expensive services. The adage "If you don't know what the product is, you are the product" will be truer than ever. This blog post explores how the utopia we're designing could quickly become a dystopia without privacy.

The second group is corporate users. The Obscuro core team being ex-R3, discovered early through building the leading consortium of global banks that privacy of sensitive trading details between counterparties is not a nice-to-have; it's mandatory. This requirement underpinned the "need to know" philosophy of R3's Corda. So far, corporate users have been slow to transact on Ethereum, despite the attraction of its innovation

culture, and Obscuro believes that making an Ethereum network confidential will unleash a new category of business applications.

The third group is a set of applications which can't work if the smart contracts don't hold secrets. Until now, Ethereum contracts have had autonomy and agency; end-users can send Ether and ERC20 token value to a smart contract, and this contract determines how to distribute that value. With Obscuro, contracts now also hold secrets in the way human agents can, and have the power to surprise users. For example, an Obscuro contract can determine if an NFT can "shape-shift" or change shape based on external events such as a full moon, or be used to manage the game board of an interactive game in a way which prevents players from "seeing round the corner" or otherwise cheating.

Team

Obscuro's core team is part of the team that built Corda, regarded as the world's most successful enterprise blockchain platform. Corda is used by the world's leading banks, financial institutions, insurance institutions and telecommunications.